UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,834	03/12/2002	Thomas Breitbach	P-44 MG	1508

28752 7590 03/15/2007
LACKENBACH SIEGEL, LLP
LACKENBACH SIEGEL BUILDING
1 CHASE ROAD
SCARSDALE, NY 10583

EXAMINER	
LU, ZHIYU	
ART UNIT	**PAPER NUMBER**
2618	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/936,834	BREITBACH ET AL.	
	Examiner	Art Unit	
	Zhiyu Lu	2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 20-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 20-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 06/26/2006 have been fully considered but they are not persuasive.

Regarding to the amended claim 1, Applicants have argued that Hultgren teaches a tele/data-communications payment method and apparatus, which is different from HBCI where HBCI provides more security and banking functions. However, Hultgren teaches a transmission path structure between a SIM card and a banking server where a Telepay gateway is in between doing transformation and processing. The only difference between claim 1 and Hultgren's invention is having a HBCI gateway instead of a Telepay gateway. For a Telepay gateway, it may not do as much banking services as HBCI does, but it involves banking transaction services. It makes clear that online banking service via GSM mobile telephone already existed at that time. And HBCI is a well-known online banking standard in the European market with its gaining popularity with providing more banking functions and support in multibanking, platform independent, and encryption and signatures for chip card. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to replace the Telepay gateway of Hultgren with HBCI gateway, in order to provide an alternative and more compatible banking service with respect to European market.

As referring to claim 21, and claim 1 too, a relevant reference, "At the Coal-face Between Financial Industries and Politics: An Interview with the Financial Issues Working Group's Chairman Charles Goldfinger" in June 1998 discloses national Internet banking standard such as HBCI in Germany and also IT infrastructure migration to Internet standard where Internet GSM

banking becomes available (page 5), which shows a common knowledge of compatibility in using HBCI with mobile network. According to definition, HBCI is designed for Internet banking with chip card. And Hultgren teaches using a GSM chip card to do online banking via a transaction gateway, where compatibility is presented. Thus, it would have been obvious to one of ordinary skill in the art to provide compatibility between HBCI and GSM network in light of modified method of Hultgren.

Regarding claim 24, Applicants have argued that the HBCI Interface Specification only teaches one security protocol, which is between the bank and the customer. However, GSM has its own security protocol too (column 12 line 59 to column 13 line 63). Thus, there is one between HBCI gateway and the bank and another one between GSM and the HBCI gateway.

Regarding claim 25, Applicants have argued that neither Hultgren nor the HBCI Interface Specification teaches that the second security protocol corresponds to a protocol reduced in terms of data quantity. However, this is an obvious case. The second security protocol between the HBCI gateway and a SIM card only deals with a single data transmission. But the second security protocol between the HBCI gateway and the bank deals with numerous data transmissions from different terminals such as mobile phones or computers. Thus it is obvious that the second security protocol handles less data quantity than the first security protocol.

Regarding claim 27, Applicants have argued that neither Hultgren nor the HBCI Interface Specification teaches the key (Ksms) is generated in the SIM by entering an initialization PIN. However, the HBCI Interface Specification discloses the key consists of several different components, where an initialization PIN (User ID assigned by bank) is one of them (VI.3). This means the generation of the key for the use of a SIM needs entering an initialization PIN.

Note: Applicants have argued that an online definition of HBCI to be a reference used in claim 1 and an interview summary to be a reference used claim 21. However, the Examiner has never disclosed the online definition and interview summary to be references in the rejections of claims 1 and 21. The Examiner only use them in the response to Applicants' arguments to indicate the definition of HBCI and its well known usage, which explains the obviousness rejections on claims 1 and 21 in sight of one of ordinary skill in the art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-23 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391).

Regarding claim 1, Hultgren teaches a method for using standardized bank services via mobile radiotelephone, comprising the steps of transmitting between a bank server and a mobile station builds on a transmission method:

inserting an Telepay gateway (30 of Fig. 1A) into the Telepay transmission path between the bank server (80 of Fig. 1A) and the mobile station (60 of Fig. 1A), which carries out a

transformation between the Telepay transmission method used at the bank end and a transmission method used at the radiotelephone end (column 3 line 39 to column 4 line 47); and

splitting of the customer-end system into two components, a SIM card of the mobile station and the Telepay gateway (Fig. 1A, column 12 line 59 to column 13 line 21).

But, Hultgren does not expressly disclose the transmission path and the gateway being HBCI transmission path and HBCI gateway.

The Examiner takes "Official Notice" that the claimed limitation is well known in the art. HBCI is a commonly known standardized bank software system used in the European market, which provides support for multibanking, platform-independent, and DES- and RSA-encryption and –signatures for chip card, which would have been obvious to one of ordinary skill in the art at the time the invention was made to migrate the system to HBCI for alternative banking service with some European market share.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hultgren into having HBCI as standard, in order to have alternative banking service with some European market share.

Regarding claim 37, Hultgren teaches a method for using standardized bank services via mobile radiotelephone, comprising the steps of

transmitting data between a bank server (80 of Fig. 1A) and a mobile station (60 of Fig. 1A) builds on a Telepay transmission method (Fig. 1A);

inserting an Telepay gateway (30 of Fig. 1A) into the transmission path between the bank server and the mobile station, which carries out a transformation between the Telepay

transmission method used at the bank end and a transmission method used at the radiotelephone end (column 3 line 39 to column 4 line 47);

splitting the customer-end Telepay system into two components, a SIM card of the mobile station and the Telepay gateway (Fig. 1A, column 12 line 59 to column 13 line 21);

forming two transmission routes, the first between a SIM card and the Telepay gateway and the second between the Telepay gateway and a bank server (Fig. 1A, column 12 line 59 to column 13 line 21); and

But, Hultgren does not expressly disclose the transmission path and the gateway being HBCI transmission path and HBCI gateway; and unpacking an HBCI protocol by the HBCI gateway and converting its protocol sequence such that compatibility with a GSM SIM card and a GSM network is obtained so that an exchange of the converted protocol with the GSM SIM card is possible.

However, HBCI is a commonly known standardized bank software system used in the European market, which provides support for multibanking, platform-independent, and DES- and RSA-encryption and –signatures for chip card, which would have been obvious to one of ordinary skill in the art at the time the invention was made to migrate the system to HBCI for alternative banking service with some European market share. And in light of the migration, compatibility between the system and apparatus is obvious to one of ordinary skill in the art to make ready for successful running of the system.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hultgren into having HBCI as standard, in order to have alternative banking service with some European market share.

Regarding claim 20, Hultgren teaches the limitation of claim 1.

Hultgren also teaches wherein two transmission routes are formed, first between a SIM card and the HBCI gateway and second between the HBCI gateway and a bank server (Fig. 1A of Hultgren).

Regarding claim 21, Hultgren teaches the limitation of claim 1.

In light of the modified method of Hultgren, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have an HBCI protocol is unpacked by the HBCI gateway and its protocol sequence is converted such that compatibility with a GSM SIM card and a GSM network is obtained in order for an exchange of the converted protocol with the GSM SIM card is to be possible.

Regarding claim 22, Hultgren teaches the limitation of claim 1.

Hultgren also teaches a carrier service for the information exchange to be short message service (column 13 lines 22-32), which would have been obvious to one of ordinary skill in the art to use it for the information exchange between HBCI gateway and mobile station serves a GSM data transmission service in the modified method of Hultgren.

Regarding claim 23, Hultgren teaches the limitation of claim 20.

Hultgren also teaches on both routes a cryptographic security is realized (column 6 lines 38-43, column 12 lines 59-65).

Regarding claim 36, Hultgren teaches the limitation of claim 1.

Hultgren also teaches an additional authentication of a subscriber takes place via an identification of his/her mobile connection to carry out an evaluation of a calling line identification (CLI) (column 13 lines 33-49).

3. Claims 24-28, 30-31 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of HBCI Interface Specification (http://www.hbci-zka.de/english/documents/specification_english/Coll_HBCI21e.pdf).

Regarding claim 24, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose wherein between the bank server and the HBCI gateway a security protocol defined by HBCI is applied and between the HBCI gateway and a SIM card a second security protocol is employed.

HBCI Interface Specification (HBCI IS) teaches the limitation of between bank server and HBCI gateway the security protocol defined by HBCI is applied and between HBCI gateway and SIM card a second security protocol is employed (III.1.3), where the first security protocol between HBCI gateway. And GSM SIM card has its own security protocol between the network and the SIM card itself (column 12 line 59 to column 13 line 63), which is between the HBCI gateway and the SIM card.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate security protocol of HBCI in transmission routes taught by HBCI

Interface Specification along with SIM card's existed security protocol into the method of Hultgren, in order to enhance information security protection on both ends.

Regarding claim 25, Hultgren and HBCI IS teach the limitation of claim 24.
The combination of Hultgren and HBCI Interface Specification teach the second security protocol corresponds to a protocol reduced in terms of data quality where the transmission only deals with a single customer, but equivalent to HBCI in terms of security technology (III.1.3), where customer chooses the encryption algorithm to be used, wherein the encryption algorithm is supported by the bank and fit for security procedure and compression procedure of HBCI.

Regarding claim 26, Hultgren and HBCI IS teach the limitation of claim 25.
HBCI Interface Specification teaches a cryptographic key (Ksms) (signature key) specific to each subscriber is securely generated and stored in a SIM card (Chip card of Fig. 1) for use in the second security protocol (I Introduction, VI.3.1.1 Key types) after regular SIM card personalization.

Regarding claim 27, Hultgren teaches the limitation of claim 1.
But, Hultgren does not expressly disclose the generation of the key (Ksms) specific to the subscriber is generated in the SIM card by entering an initialization PIN on the mobile telephone.
HBCI Interface Specification teaches the limitation of the generation of the key (Ksms) specific to the subscriber is generated in the SIM card by entering an initialization PIN (User ID) on the

mobile telephone (VI.3), where using two or more keys to generate a specific key is also well known in the art of crytography.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating key with entering initialization PIN taught by HBCI Interface Specification into the method of Hultgren, in order to generate a reliable concrete key instead of random generation.

Regarding claim 28, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the subscriber is informed per PIN letter by the bank of a PIN for generating the key (Ksms) (VI.3.1.3.2 Initial key distribution, in writing from the bank).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate informing subscriber PIN number in letter by the bank taught by HBCI Interface Specification into the method of Hultgren, in order to inform subscriber security generating PIN in a more securable way.

Regarding claim 30, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose before subscription to a service a subscriber receives the data of his bank including an initialization PIN.

HBCI Interface Specification teaches before subscription to a service the subscriber receives the data of his bank including an initialization PIN (User ID of III.1.1, VI.3.1.3.2 Initial key distribution)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate providing user an initialization PIN from his bank taught by HBCI Interface Specification into the method of Hultgren, in order to enable user to use service with security.

Regarding claim 31, Hultgren and HBCI IS teach the limitation of claim 30.
HBCI Interface Specification teaches a cryptographic method of generating the key through triple DES using country code (local PIN), bank code (routing number), user ID (account number), key type, key number, and version number (VI.3.1.1, II.5.3.2), which means during the initialization of an application, i.e. during subscription, with the aid of the KIV from initialization PIN, the key Ksms is generated through triple DES using the local PIN, the bank routing number and an account number.

Regarding claim 34, Hultgren teaches the limitation of claim 1.
But, Hultgren does not expressly disclose the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of an initialization PIN exchanged in writing.
HBCI Interface Specification teaches the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of the initialization PIN exchanged in writing (VI.3.1.3.2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the initialization PIN exchange in writing into the method of Hultgren, in order to provide official and authentic PIN exchange.

4. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of HBCI Interface Specification (http://www.hbci-zka.de/english/documents/specification_english/Coll_HBCI21e.pdf) and Fujioka (JP10-242957).

Regarding claim 32, Hultgren and HBCI IS teach the limitation of claim 27.

But, Hultgren and HBCI IS do not expressly disclose the limitation of for the generation of the Ksms in the HBCI gateway an initialization PIN is transferred to the gateway operator.

Fujioka teaches the limitation of transferring a initial key to server for generating another key (abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate transferring initialization PIN to server for generating a key taught by Fujioka into the modified method of Hultgren and HBCI IS, in order to authenticate key generation for the right client.

5. Claims 29 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of Atalla (US Patent#4288659).

Regarding claim 29, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose during a card personalization by the mobile telephone network operator together with the bank application, an initialization key KIV, derived from a master key and a SIM card-individual number, for generating a Ksms specific to the subscriber is applied onto a plurality of SIM cards.

Atalla teaches generating an initialization key based on a secret code (master key) known by both authorized individual and the bank and an identification of the terminal for generating the session key specific to the terminal user (column 1 line 45 to column 2 line 27), where applying the key generating method is obvious to one of ordinary skill in the art to apply on other cards as well.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key from a master key and a hardware individual number taught by Atalla into the method of Hultgren, in order to provide both user and hardware authentication in initialization.

Regarding claim 33, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the generation of an initialization PIN takes place at the HBCI gateway and this is transferred to the bank server.

Atalla teaches the generation of the initialization PIN takes place at the terminal (mid-node between user and bank) and data terminal must be initialized in the first operating cycle (column 1 line 45 to column 2 line 27, column 2 lines 64-67).

Considering the connection between the user and the bank, it would have been obvious to one of ordinary skill in the art to recognize that the gateway is the mid-node authentication process for

the user to proceed first before getting to the bank. The gateway would be the one who masters connections with the user and the bank. The gateway would be the first node to authenticate user and to initialize session. Thus, it would have been obvious to one of ordinary skill in the art to recognize that it is convenient and secure for the gateway to generate initialization PIN and then transfer it to the bank so that the bank can inform user the initialization key since the bank is the one who authorize the service.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key in mid-node taught by Atalla into the method of Hultgren and modify into transferring the generated initialization key to the bank, in order to provide secured user initialization and authentication in the HBCI gateway.

6. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of Elgamal et al. (US Patent#5657390).

Regarding claim 35, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged.

Elgamal et al. between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged (column 7 lines 41-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate exchanging master key taught by Elgamal et al. into the method of

Hultgren, in order for both client and server to produce session keys that would be employed to actually encrypt/encrypt data.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zhiyu Lu whose telephone number is (571) 272-2837. The examiner can normally be reached on Weekdays: 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on (571) 272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Zhiyu Lu
March 1, 2007

NAY MAUNG
SUPERVISORY PATENT EXAMINER